



ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Allison Knight, Staff Counsel
Electronic Privacy Information Center (EPIC)

Hearing on

The Truth in Caller ID Act of 2007, S. 704

Before the

Committee on Commerce, Science and Transportation
U.S. Senate

June 21, 2007
253 Russell Office Building

Chairman Inouye, Vice Chairman Stevens, and Members of the Committee, thank you for the opportunity to testify today on caller ID spoofing and the Truth in Caller ID Act of 2007, S. 704. My name is Allison Knight and I am Staff Counsel and Director of the Privacy and Human Rights Project at the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C. that seeks to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

Two separate and important privacy interests meet in the issue of caller ID spoofing. First, there is the right of callers to limit the disclosure of their phone numbers in order to protect their privacy, and in some cases, their safety. Second, there is the right for call recipients to be free from pretexting and other fraud that can lead to the loss of their privacy, and the threats of stalking, identity theft, and harassment.

The Truth in Caller ID Act of 2007, S. 704, as currently drafted does not adequately protect both interests. EPIC recommends that any ban on caller ID spoofing include an intent requirement, so that spoofing is only prohibited where it is clear that the person who does not provide identifying information “intends to defraud or cause harm.” EPIC recommended the inclusion of an intent requirement in testimony on a similar bill introduced in the House last year,¹ and this intent requirement was incorporated into the version of bill that recently passed in the House.² As Marc Rotenberg, Executive Director

¹ The Truth in Caller ID Act of 2006, H.R. 5126.

² The intent requirement was also included in the Truth in Caller ID Act of 2007, H.R. 251. EPIC testified on this House bill on February 28, 2007, in support of the intent requirement. The Truth in Caller ID Act of 2007, H.R. 251 passed the House on June 12,

of EPIC stated, an intent requirement preserves the privacy rights of callers and permits legitimate uses of spoofing, while outlawing fraud and harassment assisted by the technology.³ We also have concerns about the provision in the Senate bill that permits law enforcement agencies to possibly misrepresent their identities in the context of telecommunications services.

Telephone Customers Have Legitimate Reasons to Withhold Their Phone Numbers

The introduction of caller ID services and the associated Automatic Number Identification (ANI) created new risks to privacy. Before these services were offered, telephone customers generally had the ability to control the circumstances under which their phone numbers were disclosed to others. In many cases, there was little need for a telephone customer to disclose a personal phone number if, for example, a person was calling a business to inquire about the cost or availability of a product or wanted information from a government agency. In other cases, there was a genuine concern that a person's safety might be at risk. For example, women at shelters who were trying to reach their children were very concerned that an abusive spouse not be able to find their

2007, and was received into the Senate and referred to the Committee on Commerce, Energy and Transportation on June 13, 2007.

³ *H.R.5126, the Truth in Caller ID Act of 2006: Before the Subcomm. on Telecommunications and the Internet of the H. Comm. on Energy and Commerce, 109th Cong. (2006)* (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center). *See also, H.R.251, the Truth in Caller ID Act of 2007: Before the Subcomm. on Telecommunications and the Internet of the H. Comm. on Energy and Commerce, 110th Cong. (2007)* (statement of Allison Knight, Director, Privacy and Human Rights Project, Electronic Privacy Information Center).

location.⁴

In the context of the Internet and the offering of voice services over Internet Protocol (VOIP), there are additional concerns about the circumstances under which a person may be required to disclose their identity. The Supreme Court has repeatedly made clear that the right to be anonymous is protected by the First Amendment and also that the Internet is entitled to a high level of First Amendment protection.⁵

Many individuals have legitimate reasons to report a different number than the one presented on caller ID. For example, a person may wish to keep her direct line private when making calls from within an organization. Such an arrangement legitimately gives call recipients a number to which they can return a call, but prevents an individual person's phone from being inundated with calls that should be routed elsewhere.

In addition to threatening a person's rights to privacy and to freedom of speech, in some circumstances disclosure of a person's phone number may also put his or her safety at risk. For example, domestic violence survivors, shelters, and other safe homes need to preserve the confidentiality of their phone numbers. They may need to contact abusers without exposing their location, in order to arrange custody or other legitimate matters. They may need to contact businesses the abuser is acquainted with, and that may share survivor information with the abuser. They may also need to contact other third parties, such as businesses that have permissive privacy policies, and thus share collected

⁴ Letter from National Network to End Domestic Violence to the House Committee on Energy and Commerce (May 16, 2006).

telephone numbers with list or data brokers. In all of these situations, preserving anonymity is necessary for safety.⁶

Caller ID Blocking Does Not Adequately Protect Privacy Interests

Caller ID blocking may seem like a viable means for allowing callers to protect their anonymity while not misleading recipients. However, caller ID blocking is not a complete solution. One reason for this is that caller ID is not the only way that a caller can be identified. Another system, known as Automatic Number Identification, or ANI, will still disclose a caller's identity in many situations, regardless of whether or not the caller used call blocking. This means that many businesses, emergency service providers, and anyone with a toll-free number can reliably gain the phone number of a caller, even if caller ID is blocked. Spoofing services can protect the anonymity of a caller's ANI data when calling toll-free numbers and those entities that use ANI identification.

Some recipients prevent blocked ID calls, and indications are that the number of individuals doing this is growing. In the case of a domestic violence survivor attempting to safely reach a required phone number, an individual would have to use spoofing for the innocent purpose of preserving the confidentiality of his or her number.

We also cannot ignore the privacy interests of those who decline to accept calls from unknown numbers. If an individual has been habitually harassed by calls from a

⁵ *Watchtower Bible & Tract Society v. Village of Stratton*, 536 U.S. 150 (2002), *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), and *Talley v. California*, 362 U.S. 60 (1960); *ACLU v. Reno*, 521 U.S. 844 (1997).

caller-ID blocked number, we should not permit the harasser to use spoofing as a means to circumvent the individual's screening. At the same time, it is clear that there could be prosecution for harassment whether or not additional prohibition on spoofing were enacted.⁷

Spoofing Can Create Privacy Risks

This is not to say that caller ID spoofing is an unqualified good -- far from it. Last year, EPIC brought to Congress's attention the problem of pretexting consumers' phone records.⁸ Pretexting is a technique by which a bad actor can obtain an individual's personal information by impersonating a trusted entity. Pretexters have spoofed the telephone numbers of courthouses, in order to harass people for supposedly missing jury duty, threatening fines or arrest unless they turn over Social Security numbers or other personal information.⁹ Rob Douglas of PrivacyToday.com, with whom EPIC has worked on the pretexting issue, noted how fraudsters would use spoofing services in order to fool

⁶ *Domestic Violence and Privacy*, Electronic Privacy Information Center
<http://www.epic.org/privacy/dv/>.

⁷ See 47 U.S.C. § 223; 47 U.S.C. § 227.

⁸ *Protecting Consumers' Phone Records: Before the Subcomm. on Consumer Affairs, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center).

<http://www.epic.org/privacy/iei/sencomtest2806.html>; *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?: Before the H. Comm. on Energy and Commerce*, 109th Cong. (2006) (statement of Marc Rotenberg, President and Executive Director, Electronic Privacy Information Center)
http://www.epic.org/privacy/iei/pretext_testimony.pdf.

⁹ Sid Kirchmeyer, *Scam Alert: Courthouse Con*, AARPBulletin, May 2006,
http://www.aarp.org/bulletin/consumer/courthouse_con.html.

customers into thinking that fraudulent calls were coming from trusted sources.¹⁰

For these reasons, illegitimate spoofing activities should be curtailed. Law enforcement and telephone companies can retrace these calls to the originating service.¹¹ A spoofed number is not completely anonymous and without accountability. Preventing spoofing for harmful reasons will hold illegitimate spoofers accountable.

Intent Requirement

The inclusion of an intent requirement in the Senate bill would focus the punishment on harmful and fraudulent uses of caller ID spoofing while preserving legitimate uses of the technique. In addition, an intent requirement would render specific exemptions for law enforcement unnecessary, as legitimate law enforcement activity that employs spoofing would be protected by the requirement to show intent to defraud or cause harm.

Significance of NSA Surveillance Program for Privacy of Call Records

Mr. Chairman, I would also like to bring to the Committee's attention our concern that the National Security Agency may have constructed a massive database of telephone toll records of American consumers. Last year, EPIC filed a complaint with the Federal Communications Commission in which we alleged that Section 222 of the Communications Act, which protects the privacy of customer record information, might

¹⁰ *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?: Before the H. Comm. on Energy and Commerce, 109th Cong. (2006)* (statement of Robert Douglas, CEO, PrivacyToday.com), <http://www.privacytoday.com/HC020106.htm>.

have been violated.¹² We urged the Commission to undertake an investigation of this issue. In light of the ongoing controversy about the possibility that federal privacy laws were violated, the need to pursue this investigation is clear.

We respectfully ask Members of this Committee to support EPIC's recommendation that the FCC undertake an investigation of the possibly improper disclosure of telephone toll records by the telephone companies that are subject to the privacy obligations contained in the Communications Act. If the Communications Act was violated, that should be of great concern to the Committee.

Conclusion

Spoofing caller ID numbers can create a real risk to individuals who might be defrauded or harmed by illegitimate uses of this technology. At the same time, it is important not to punish those who may have a legitimate reason to conceal their actual telephone numbers. The inclusion of an intent requirement in the Truth in Caller ID Act of 2007 would significantly improve the bill by distinguishing between appropriate and inappropriate caller ID spoofing.

I will be happy to answer any questions you might have at this time.

¹¹ Peter Svenson, *Caller ID Spoofing Becomes All Too Easy*, USA TODAY, Mar. 1, 2006, http://www.usatoday.com/tech/news/2006-03-01-caller-id_x.htm.

¹² EPIC Complaint to the Federal Communications Commission (May 16, 2006).